IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:
Ahmed El-Sayed Ahmed et al.
Application No. 10/555,408
Filed: November 1, 2005
Confirmation No. 9403
For: SYSTEM AND METHOD FOR DETERMINING A COMPUTER USER PROFILE FROM A MOTION-BASED INPUT DEVICE
Examiner: Simon P. Kanaan
Art Unit: 2432
Attorney Reference No. 2847-72452-01

FILED VIA EFS
ON MARCH 30, 2011

FILED VIA ELECTRONIC FILING SYSTEM
COMMISSIONER FOR PATENTS

DECLARATION OF PRIOR INVENTION UNDER 37 C.F.R. § 1.131

We, Ahmed El-Sayed Ahmed and Issa Traore, declare that we are the inventors of the subject matter recited in pending claims 1-5, 7-12, 14 and 19-31 of the referenced application. We declare that the respective subject matter of the pending claims was reduced to practice before April 2, 2003. In support of this declaration, we allege the following facts:

1. Exhibit A is a PowerPoint presentation describing the behavioral biometrics-based user verification system for use with a mouse input device constructed and tested for its intended purpose by Ahmed El-Sayed Ahmed and Issa Traore. Also described in the presentation are associated verification methods performed and tested for their intended purposes. The presentation was prepared before April 2, 2003, and thus the inventions described in the presentation were made before April 2, 2003.

2. Before April 2, 2003, a behavioral biometrics-based user verification system for use with a mouse input device having the features of claim 1 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system made and tested before April 2, 2003, comprised: a data interception unit configured to intercept

inputs from a user that are directed to an application other than a user authentication application (see, e.g., slides 12 and 27), wherein the data interception unit is configured to passively collect at least one of mouse movement data, mouse point and click data, and mouse drag and drop data generated in response to usage of the mouse in providing input to the application other than the user authentication application (see, e.g., slide 4); a behavior analysis unit operatively coupled to said data interception unit to receive the passively collected mouse data (see, e.g., slides 11, 12 and 14-18) and a behavior comparison unit operatively coupled to said behavior analysis unit (see, e.g., the User Identification Stage shown and described at, e.g., slides 12, 18-25) wherein said system dynamically monitors and passively collects behavioral biometric information, and translates said behavioral biometric information into representative data, stores and compares different results, and outputs a user identify result associated with authorization of the user (see, e.g., slides 21-25).

3. Before April 2, 2003, a user verification system having the features of claim 2 as recited in the referenced application existed and worked for it intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said system is suitably configured for real-time monitoring (see, e.g., slides 26-27).

4. Before April 2, 2003, a user verification system having the features of claim 3 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said data interception unit is configured to identify data based on mouse movement between first and second locations, wherein movement between the first and second locations is not associated with a mouse click (see, e.g., slides 4 and 5).

5. Before April 2, 2003, a user verification system having the features of claim 4 as recited in the referenced application existed and worked for it intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said data interception unit is

configured to identify data based on mouse movement between first and second locations, wherein movement between the first and second locations is not associated with a mouse click (see, e.g., slides 4 and 5).

6. Before April 2, 2003, a user verification system having the features of claim 5 as recited in the referenced application existed and worked for it intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said data interception unit is further configured to characterize movement based on at least one of average speed, average traveled distance, and direction of movement (see, e.g., slide 5).

7. Before April 2, 2003, a user verification system having the features of claim 7 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said data interception unit is further configured to identify action from a mouse as one of drag and drop, point and click, mouse movement, and silence such that in use, said system receives data from a mouse (see, e.g., slide 4).

8. Before April 2, 2003, a user verification system having the features of claim 8 as recited in the reference application existed and worked for its intended purpose (see Exhibit A). In particular, the user verification system made and tested before April 2, 2003, comprised the user verification system recited above at paragraph 2, wherein said data interception unit is further configured to characterize mouse movement based on at least one of average speed, average traveled distance, and direction of movement (see, e.g., slide 5).

9. Before April 2, 2003, a method of characterizing a user having the features of claim 9 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised: receiving at least one of mouse movement data, mouse point and click data, and mouse drag and drop data associated with movement of a computer mouse in supplying data to a user application other

than an authentication application (see, e.g., slide 4); forwarding the received data to the user application (see, e.g., slides 26 and 27); passively intercepting at least a portion of the received data and forwarding the intercepted portion to a behavioral processing unit (see, e.g., slide 12); and processing the intercepted portion so as to develop a signature for a user (see, e.g., slides 14 and 18).

10. Before April 2, 2003, a method of characterizing a user having the features of claim 10 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, further comprising comparing the signature with a signature of an authorized user (see, e.g., slides 18-25).

11. Before April 2, 2003, a method of characterizing a user having the features of claim 11 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, further comprising filtering the data after processing and before developing (see, e.g., slides 10-12).

12. Before April 2, 2003, a method of characterizing a user having the features of claim 12 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, further comprising processing the data, and developing the signature in real-time (see, e.g., slides 26 and 27).

13. Before April 2, 2003, a method of characterizing a user having the features of claim 14 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, further comprising characterizing mouse movement based on at least one of average speed, average traveled distance, and direction of movement (see, e.g., slide 5).

14. Before April 2, 2003, a user verification system having the features of claim 19 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system made and tested before April 2, 2003 comprised the system recited above at paragraph 2, wherein the behavior comparison unit is configured to store user identities for a plurality of potential users, and the user identity result identifies the user from among the plurality of potential users (see, e.g., slides 19-25).

15. Before April 2, 2003, a user verification system having the features of claim 20 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system made and tested before April 2, 2003 comprised the system recited above at paragraph 2, wherein the behavior comparison unit is configured to produce the user identity result based on mouse movement speed compared to traveled distance, average speed per direction of movement, a distribution of movement directions, average speed with respect to action type, a distribution of actions, a distribution of traveled distance, and a distribution of movement elapsed time (see, e.g., slides 4-6 and 28).

16. Before April 2, 2003, a method of characterizing a user having the features of claim 21 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the signature for the user is developed based on movement speed compared to traveled distance, average speed per direction of movement, distribution of movement directions, average speed with respect to action type, a distribution of actions, a distribution of traveled distance, and a distribution of movement elapsed time (see, e.g., slides 4-6 and 28).

17. Before April 2, 2003, a method of characterizing a user having the features of claim 22 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the passively collected behavioral biometric data is based on mouse movement between first and second locations, wherein movement between the first and second locations is not associated with a mouse click (see, e.g., slides 4 and 5).

18. Before April 2, 2003, a method of characterizing a user having the features of claim 23 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the behavioral biometric information from the mouse is obtained in a background process (see, e.g., slides 3 and 28-28).

19. Before April 2, 2003, a user verification system having the features of claim 24 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system made and tested before April 2, 2003 comprised the system recited above at paragraph 2, wherein the behavior analysis unit is configured to establish a user signature based on a plurality of sessions in an enrollment mode (see, e.g., slides 16-25).

20. Before April 2, 2003, a behavioral biometrics-based use verification system for use with a mouse input device having the features of claim 25 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system made and tested before April 2, 2003, comprised: a data interception unit configured to intercept inputs from a user that are directed to an application other than a user authentication application (see, e.g., slides 12 and 27), wherein the data interception unit is configured to passively collect at least one of mouse movement data, mouse point and click data, and mouse drag and drop data (see, e.g., slide 4); a behavior analysis unit operatively coupled to said data interception unit to receive the passively collected mouse data (see, e.g., slides 11, 12 and 14-18); and a behavior comparison unit operatively coupled to said behavior analysis unit (see, e.g., the User Identification Stage shown and described at, e.g., slides 12, 18-25), wherein said system dynamically monitors and passively collects behavioral biometric information, and translates said behavioral biometrics information into representative data, stores and compares different results, and outputs a user identify result (see, e.g., slides 21-25).

21. Before April 2, 2003, a behavioral biometrics-based use verification system for use with a mouse input device having the features of claim 26 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the system

made and tested before April 2, 2003, comprised: a data interception unit for receiving inputs from a user that are directed to an application other than a user authentication application (see, e.g., slides 12 and 27), wherein the data interception unit is configured to transparently collect at least one of mouse movement data, mouse point and click data, and mouse drag and drop data generated in response to the user (see, e.g., slide 4); a behavior analysis unit operatively coupled to said data interception unit to receive the transparently collected mouse data (see, e.g., slides 11, 12 and 14-18); and a behavior comparison unit operatively coupled to said behavior analysis unit (see, e.g., the User Identification Stage shown and described at, e.g., slides 12, 18-25) wherein said system dynamically monitors and passively collects behavioral biometric information, and translates said behavioral biometrics information into representative data, stores and compares different results, and outputs a user identify result (see, e.g., slides 21-25).

22. Before April 2, 2003, a method of characterizing a user having the features of claim 28 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the signature for the user is based on a distribution of travelled distances (see, e.g., slides 5-10).

23. Before April 2, 2003, a method of characterizing a user having the features of claim 29 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the passively collected mouse data includes mouse movement data (see, e.g., slides 4 and 5).

24. Before April 2, 2003, a method of characterizing a user having the features of claim 30 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the passively collected mouse data includes mouse point and click data (see, e.g., slides 3 and 28-28).

25. Before April 2, 2003, a method of characterizing a user having the features of claim 31 as recited in the referenced application existed and worked for its intended purpose (see Exhibit A). In particular, the method tested before April 2, 2003 comprised the method recited above at paragraph 9, wherein the passively collected mouse data includes drag and drop data (see, e.g., slides 3 and 28-28).

26. All statements made herein and of our own knowledge are true and all statements made on information are believed to be true; and further, these statements were made with the knowledge that willful false statements and like are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code, and that any such willful false statements made may jeopardize the validity of the application or any patent issuing thereon.

Mar 15, 2011

Ahmed El-Sayed Ahmed — Date

March 10/2011

Issa Traore — Date

Development of a Mouse Movement Intrusion Detector using Neural Networks

By:
Ahmed Awad E. A.
ECE Department, Uvic

Exhibit A

Contents

- Mouse Movement Detector (Introduction to the Idea)
- Proposed System Design
- Results from past experiments
- Planning for next experiment

Mouse Movement Detector

- We claim that it is possible to identify the user by analyzing his Mouse Movements dynamics over a specific period.
- Mouse Dynamics Signature can be calculated for each user, this signature will be used as a reference in the comparison process.
- Intrusion detection is a good application of this detector

Classification of Actions

- Movement (General Movement)
- Drag and Drop (the action starts with mouse button down, movement the mouse button up)
- Point & Click (mouse movement followed by a click or double click)
- Silence (No Movement)

Movement Analysis

- Examples:
  - Calculating the average speed compared to the traveled distance, this produces three graphs for the 3 types of movement actions
  - Calculating average speed compared to the movement direction, 8 different directions are considered
  - Calculation the average traveled distance for a specific period of time, with regards to different movement directions; from this data we can build a pattern for the use of different directions.

Silence Analysis

- Examples:
  - Calculating the average of silence periods between movements
  - Calculating amount of silence in a period of time
  - Comparing the percentage of the silence time to movement time in a period of time
  - Determining weights for different movement directions to answer the following question, what is the major movement direction to start movement after a silence period
  - What is the major movement direction to end with before a silence period

Experiment 1

- 4 participants only, 3 sessions per user
- All Mouse actions were recorded and analyzed
- A set of factors were calculated based on the analysis of each user behavior
- Confirming that movement direction has an effect on the recorded factors
- Checking if there is any pattern characterizing a user which can be used for the identification process

Experiment 1 - Results

User 1
Sample #1

Number of Recorded Actions: 2425
Average Speed: 272.295
Elapsed Time: 122 ~ min
Average Waiting Time: 1.4 Sec
% waiting time to elapsed time: 45.2712

User 2

Number of Recorded Actions: 1121
Average Speed: 177.78
Elapsed Time: ~ 54 min
Average Waiting Time: 1.4 Sec
% waiting time to elapsed time: 54.49

User 1
Sample #2

Number of Recorded Actions: 1043
Average Speed: 216.5
Elapsed Time: ~ 40 min
Average Waiting Time: 1 Sec
% waiting time to elapsed time: 38.98

User 3

Number of Recorded Actions: 1045
Average Speed: 284.65
Elapsed Time: ~ 55 min
Average Waiting Time: 1.4 Sec
% waiting time to elapsed time: 54.18

Experiment 1 - Results

Ahmed Sample #1

A = 297.76 N = 26.35	A = 263.72 N = 23.67
A = 229.85 N = 21.69	A = 288.29 N = 28.29

Yasien

A = 173.03 N = 30.06	A = 210.17 N = 15.70
A = 167.24 N = 24.44	A = 174.15 N = 29.79

Ahmed Sample #2

A = 258.2 N = 21.76	A = 201.3 N = 28.76
A = 195.5 N = 24.06	A = 217.8 N = 25.41

Fayed

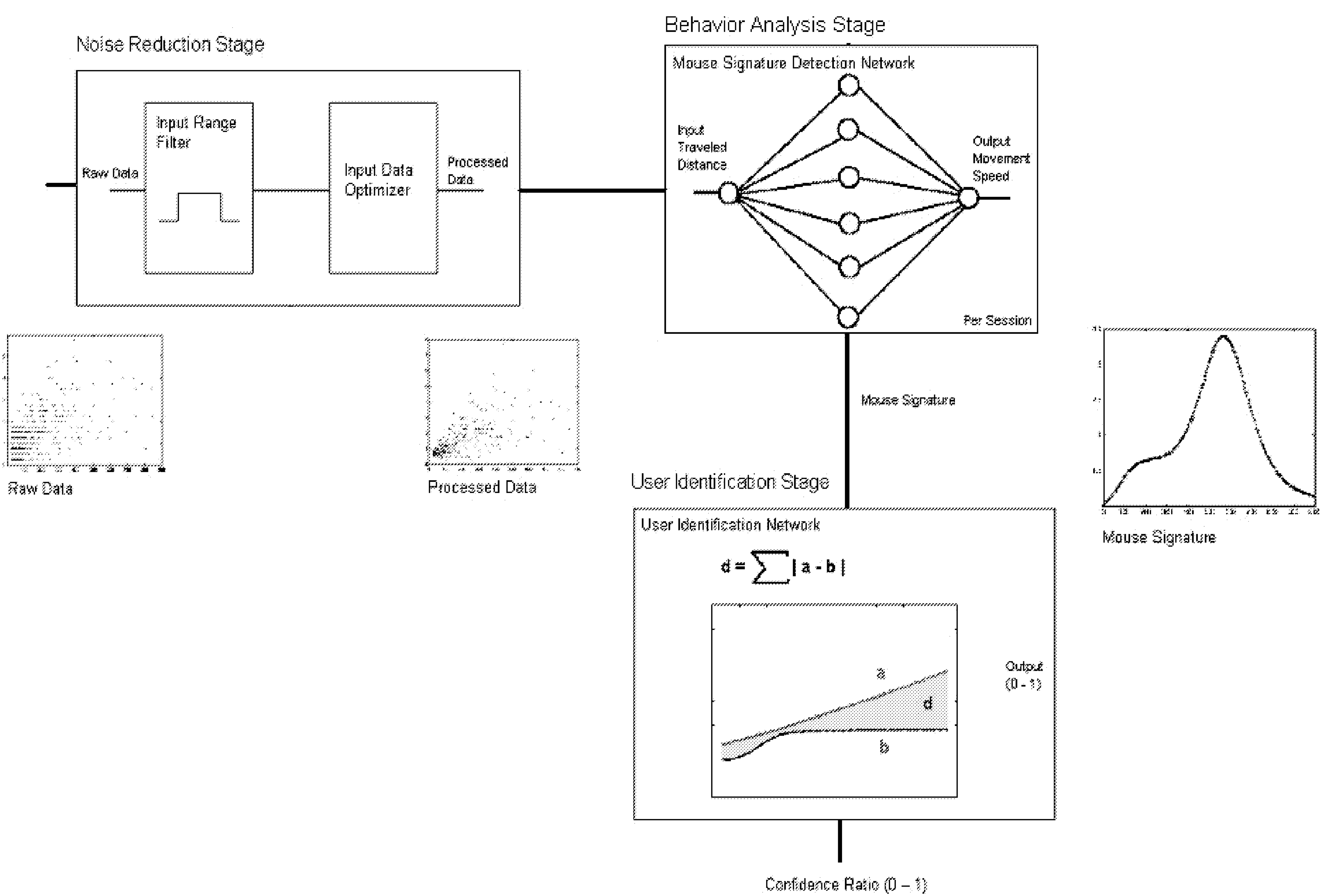
A = 358.38 N = 28.42	A = 244.346 N = 20.48
A = 280.65 N =15.31	A = 250.869 N = 35.79

Experiment 1 - Conclusions

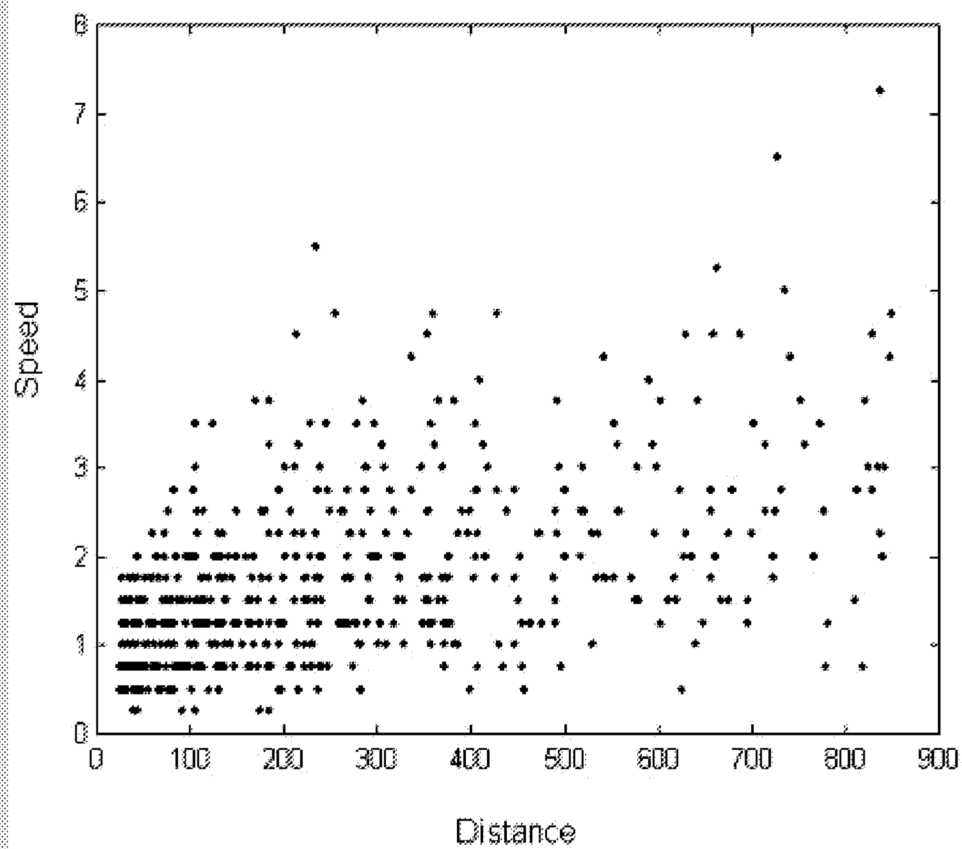
- Movement Direction is a very important factor, need to enhance the detector to support 8 directions
- Noise is high, need to work on reducing that by developing a more sensitive recording module.
- There are some similarity in the recorded factors for each user, but it is not enough for identification purpose, more work is needed either to increase the number of factors, or to develop a behavior modeling algorithm for the existing ones.

Proposed Design

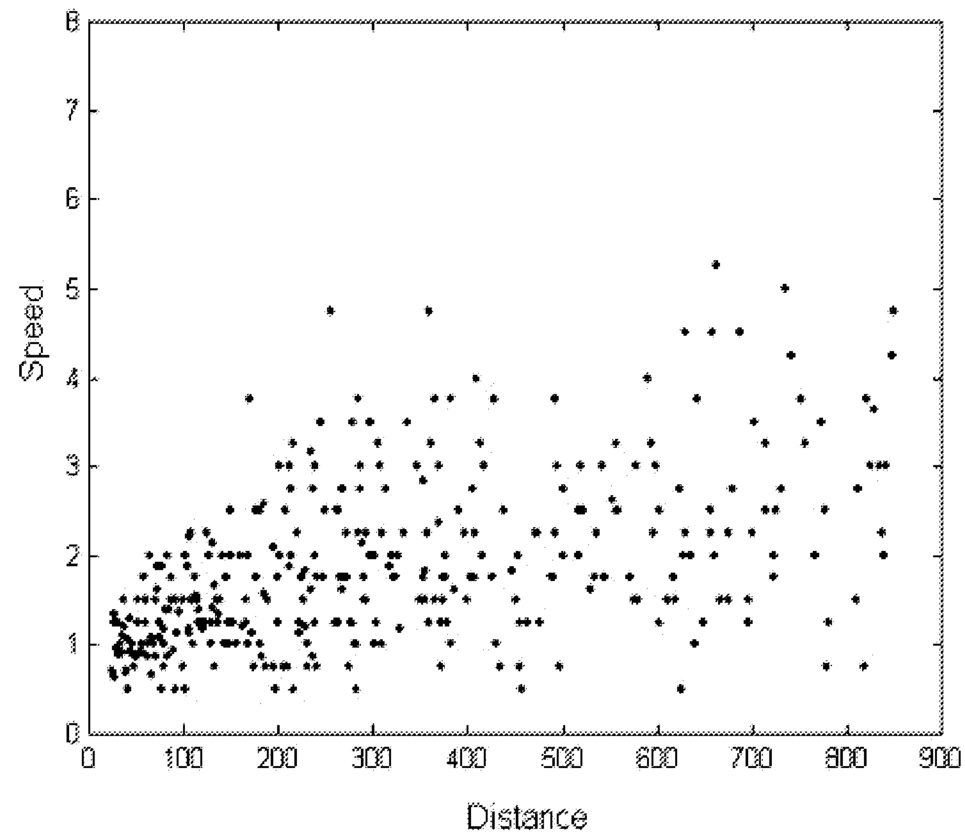
- The detector functionality can be divided into 3 stages:
  - Noise Reduction Stage
  - Behavior Analysis Stage
  - User Identification Stage


Noise Reduction Stage
Raw Data
Input Range Filter
Input Data Optimizer
Processed Data
Raw Data
Processed Data
Behavior Analysis Stage
Mouse Signature Detection Network
Input Traveled Distance
Output Movement Speed
Per Session
Mouse Signature
Mouse Signature
User Identification Stage
User Identification Network
d = ∑ | a - b |
a
d
b
Output (0 - 1)
Confidence Ratio (0 – 1)

Noise Reduction Stage



Before Filtration

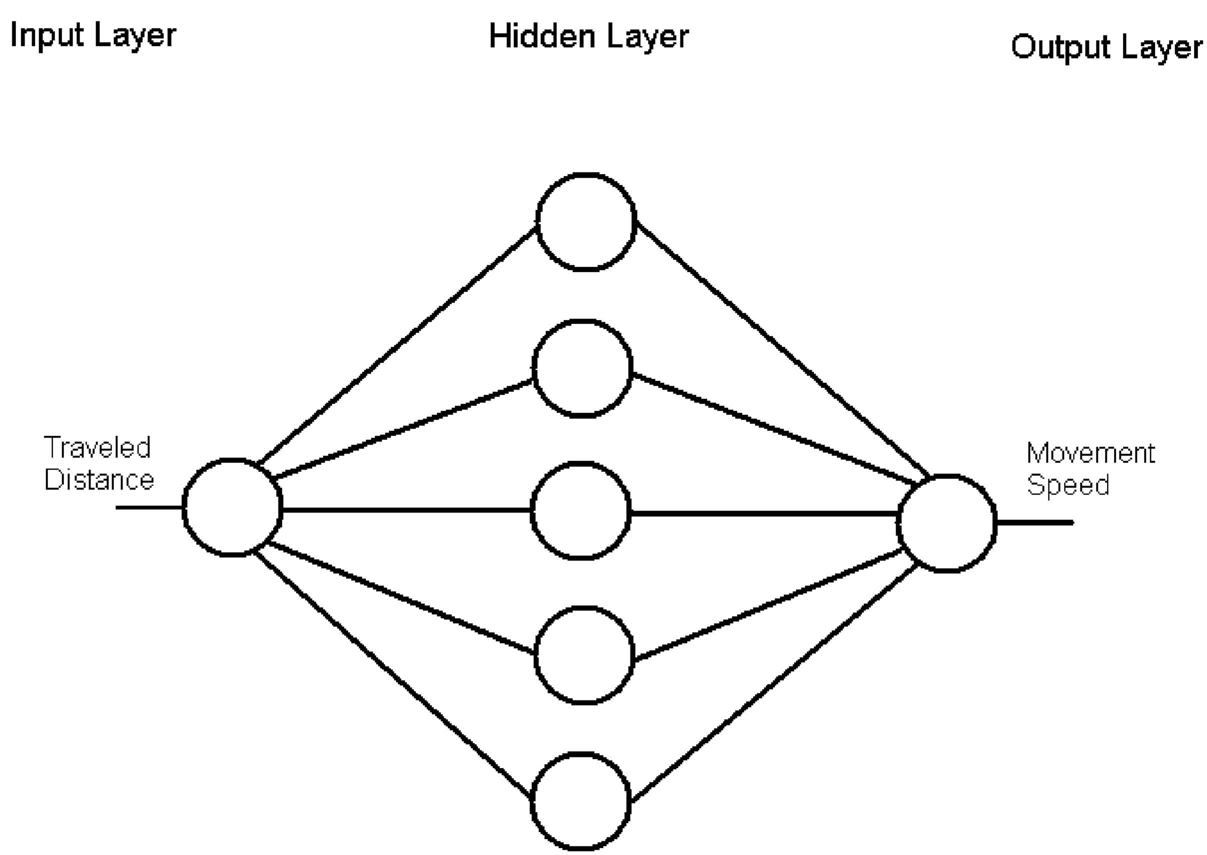


After filtration

Behavior Analysis Stage

- A Neural Network will be trained to model user behavior, represented as a relation between traveled distance and movement speed
- This is similar to using neural network for curve approximation.
- After the training is completed, will use the trained network to produce a curve representing the Mouse Movement Signature

Neural Network Model



- Multi layer perceptron, feed forward 3 Layers Network, 1 input, 1 output, and one hidden layer

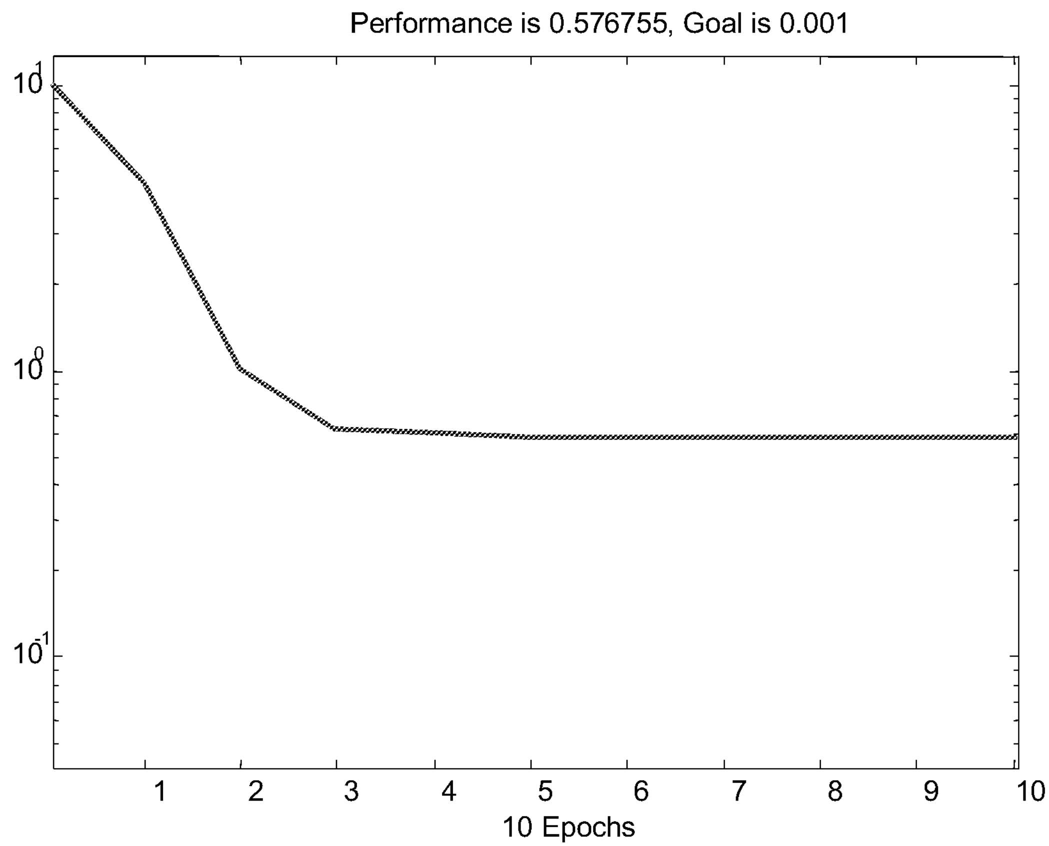
- Hidden Layer consists of 5 nodes, tuned to increase performance and prevent overfitting

- Activation function: sigmoid

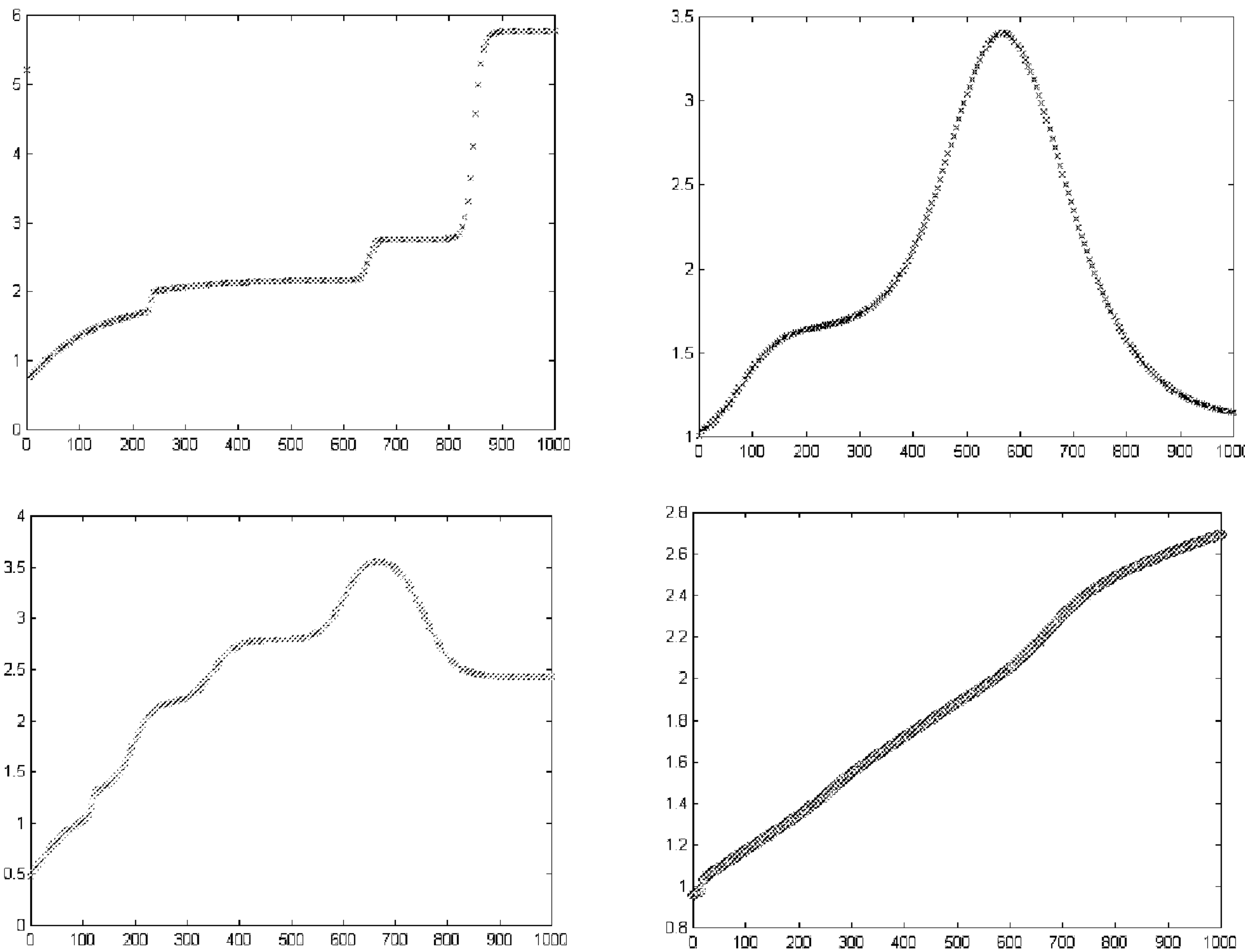
Network Training

- Back propagation algorithm is used
- The network is pre trained with a straight line input before training it with actual data
- Number of epochs is tuned to avoid over training
- Batch training is used

Learning Rate



Mouse Signature

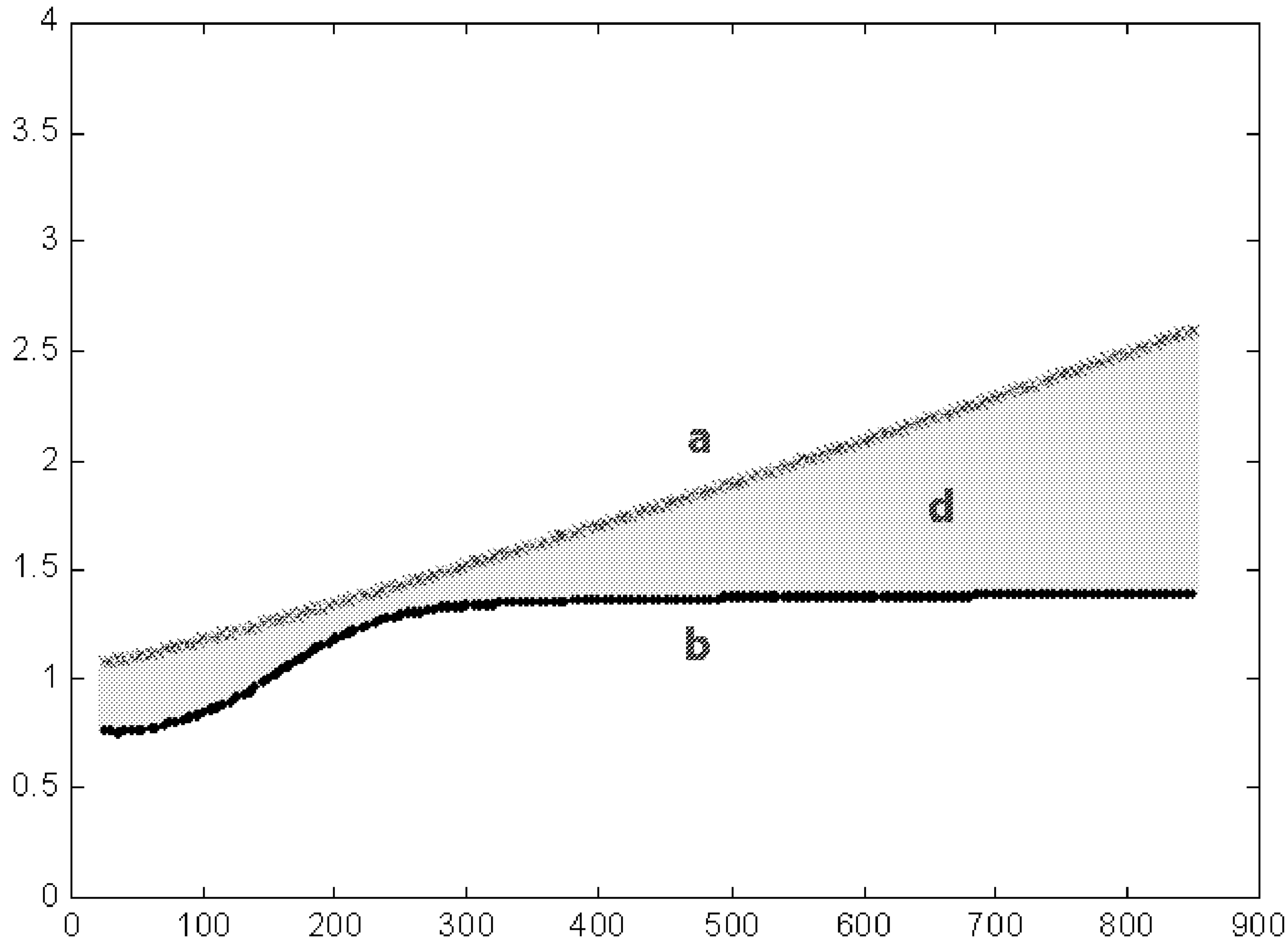


Mouse Signatures
for 4 different users

User Verification Stage

- Compares the generated mouse signature to a reference one
- A simple comparison algorithm is used to produce a factor representing the difference between the two signatures
- Confidence ratio (0 to 1) is calculated from this factor

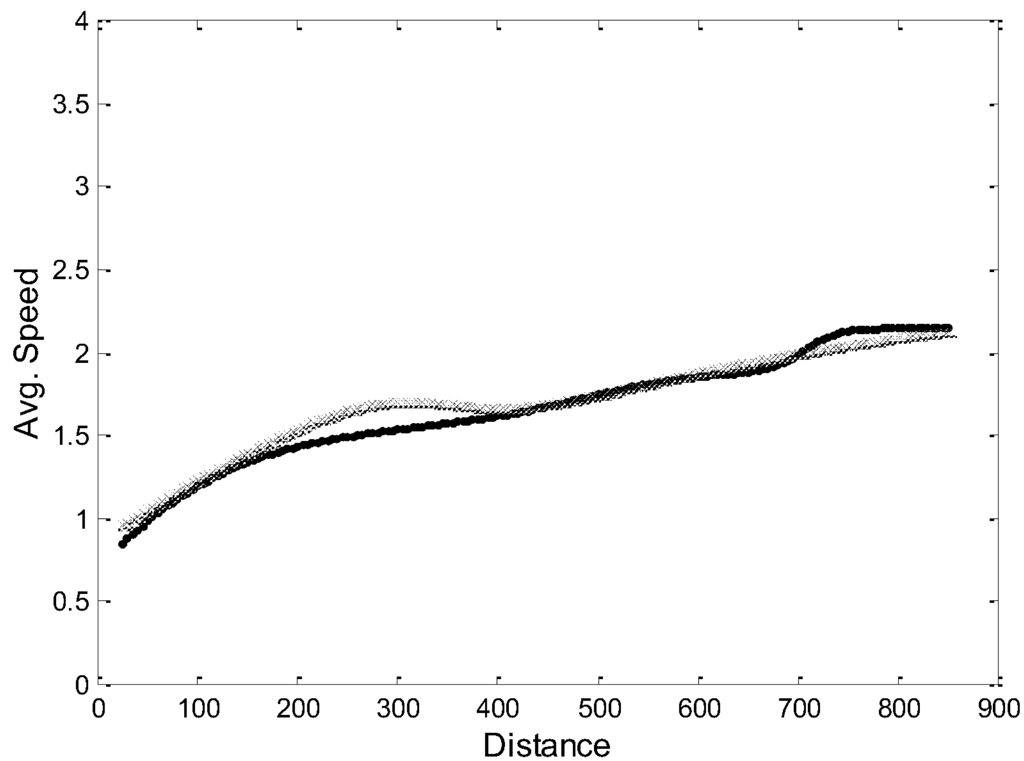
User Verification Stage



$$d = \sum |a - b|$$

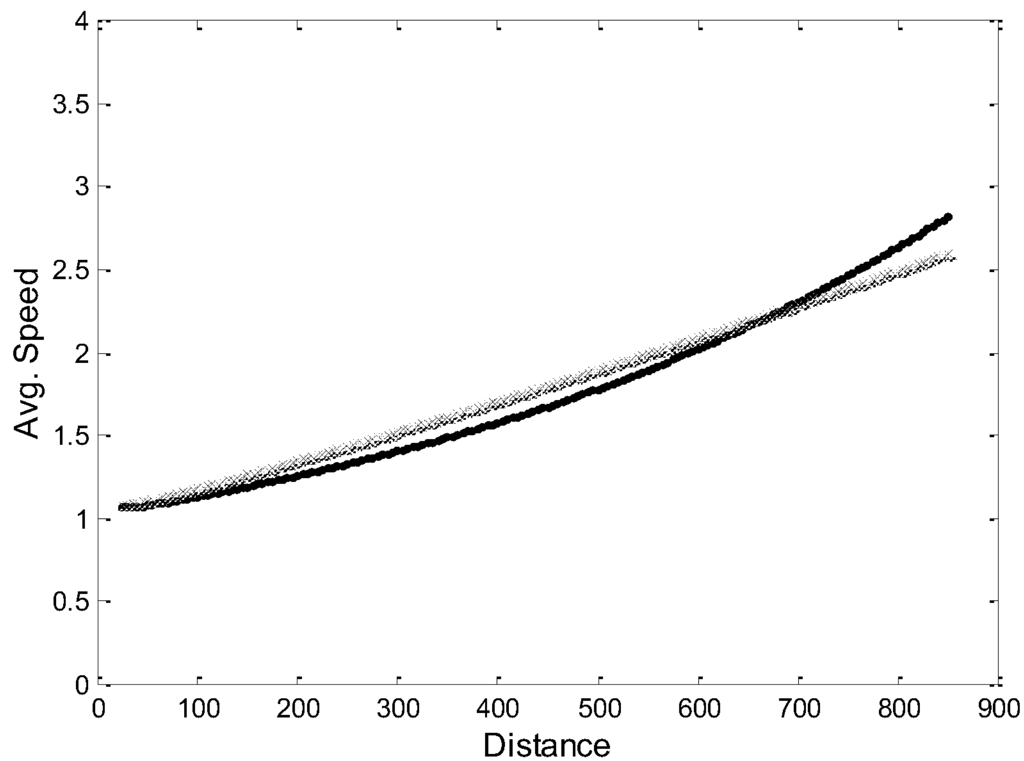
Confidence Ratio = f(d)

Experiment 2 - Results



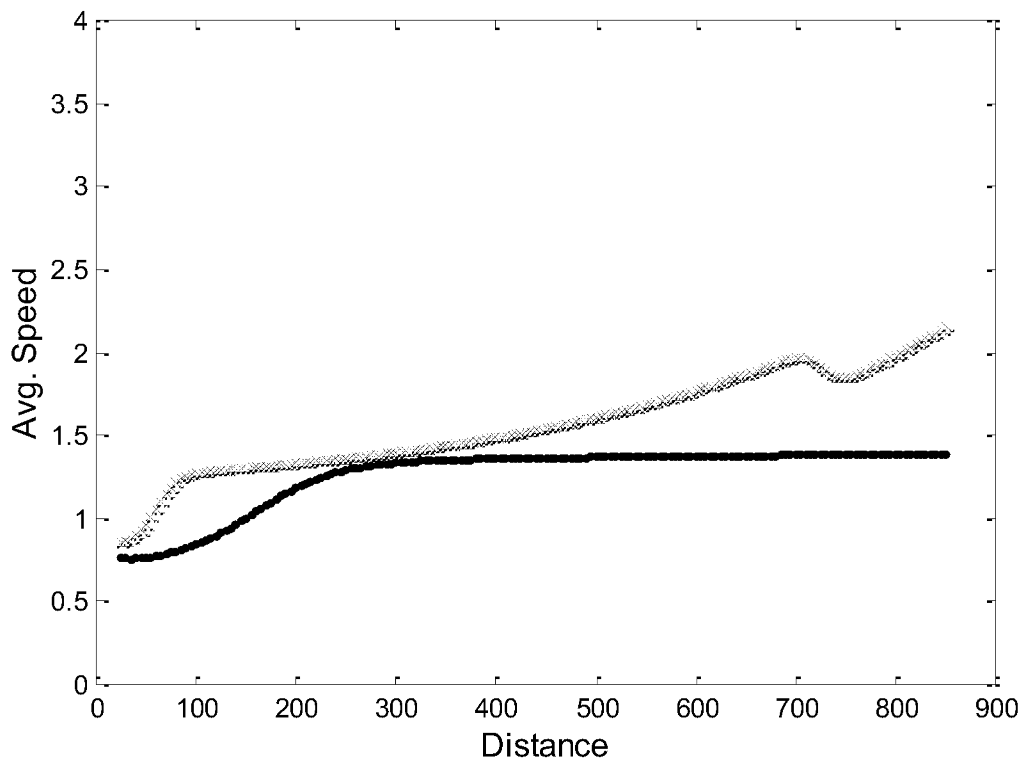
Reference	Compare to	Result
Ahmed 1	Ahmed 3	10.7561

Experiment 2 - Results



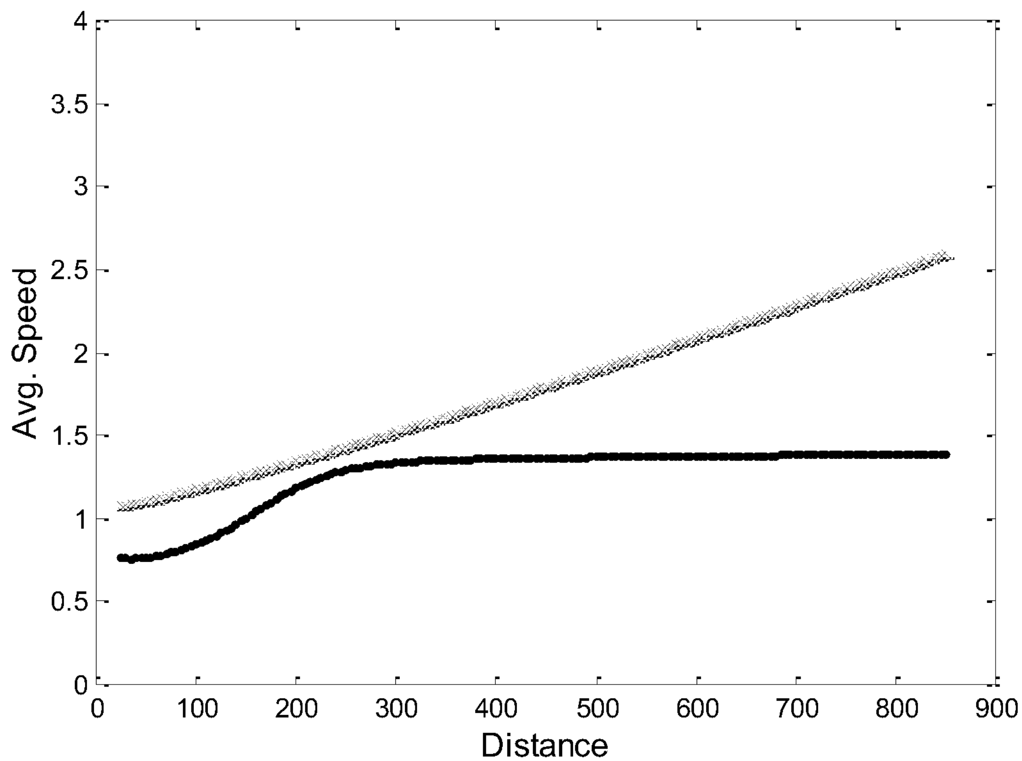
Reference	Compare to	Result
Sythuis 1	Sythuis 2	15.1333

Experiment 2 - Results



Reference	Compare to	Result
Suraya 1	Ahmed 2	51.7716

Experiment 2 - Results



Reference	Compare to	Result
Suraya 1	Sythuis 2	88.5597

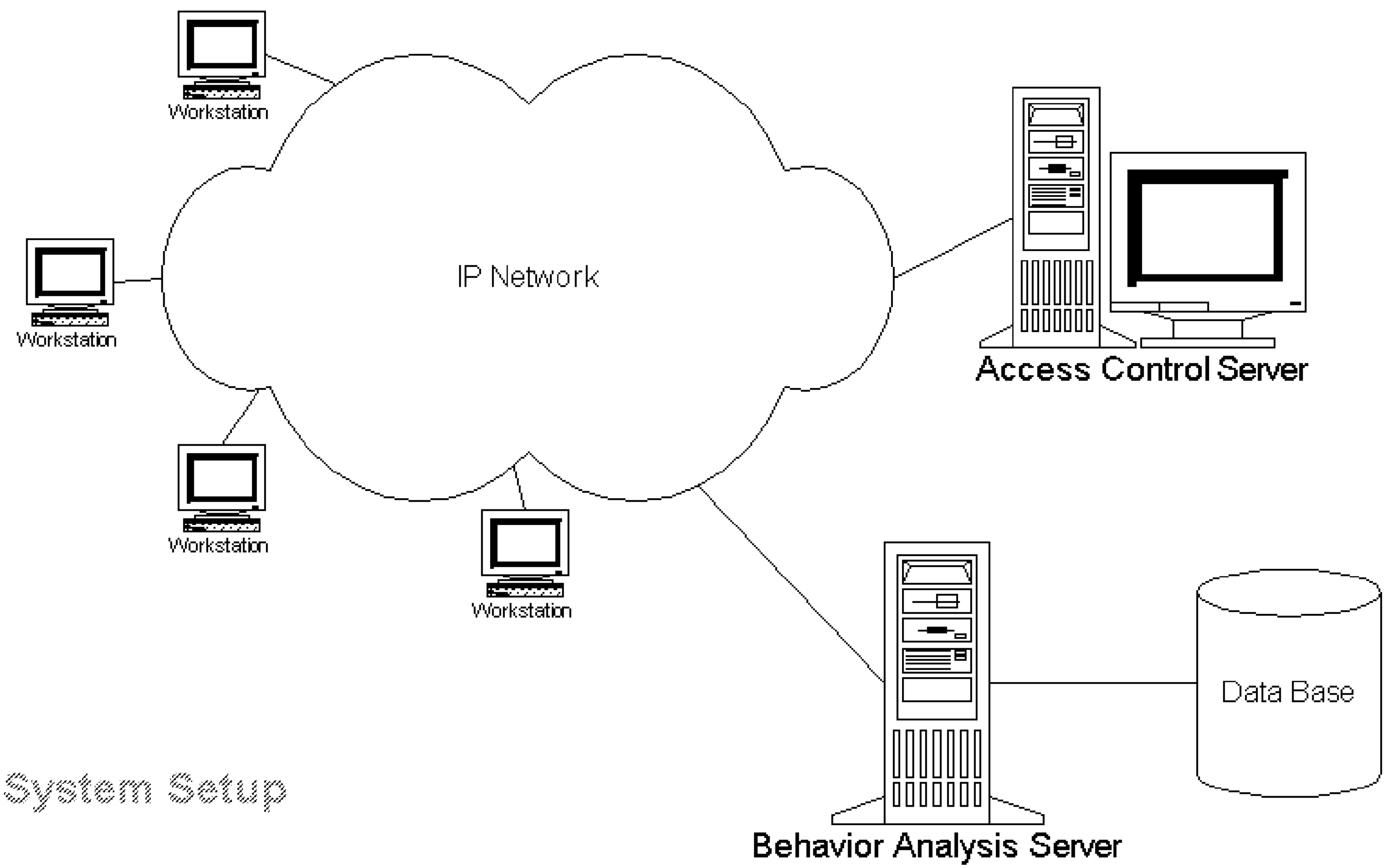
Experiment 2 - Conclusions

- It is possible to produce a curve characterizing the user behavior(Mouse Signature), this curve is reproducible through different recorded sessions.
- For the 7 participants, it was possible to identify the user by comparing his mouse signature to the recorded one.
- Threshold level should be calculated (can be per user) to reduce FAR/FRR in the verification process.
- Need to conduct more wide experiment to calculate the sensitivity and effectiveness of the proposed detector.

Experiment 3 Planning

- Targeting a number of 30 participants
- Convenient user interface, trying to link to windows account
- Behavior Analysis Server monitors active accounts on the IP network
- 14 days test period
- Expected to record about 160 session/test period per user

Experiment 3 Planning



System Setup

Experiment 3 Planning

- Calculate FAR for each user account over the recorded sessions, and if needed propose a statistics algorithm to reduce this ratio
- Determining the sensitivity of the system, how fast the system will be able detect intrusion
- This can be tuned up by increasing/decreasing the detection period
- Determining the effect of effect of including movement direction analysis on the FAR/FRR of the system

Questions

?

Thank You

Neural Network - Definition

- A neural network is a computational method inspired by studies of the brain and nervous systems in biological organisms.
- A Computing system made of a number of simple, highly interconnected processing elements, which process information by their dynamic state response to external input.

given by R.Hecht-Nielsen (1989)

Neural Network - A biological view

- Human brain is highly complex, non-linear, parallal and efficient information processing system.
- Neurons (10 billion) - structural constituents of the brain.
- Synapses (60 billion) - massive interconnections that impose excitation or inhibition.
- Axons - transmission lines
- Denderites - receptive zones

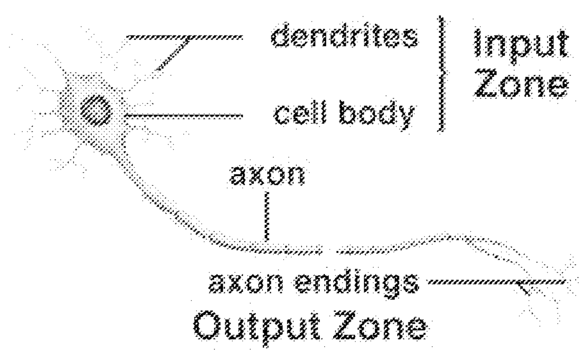
Neurons and Synapses

- The basic computational unit in the nervous system is the nerve cell, or neuron. A neuron has:
  - Dendrites (inputs)
  - Cell body
  - Axon (output)
- A neuron receives input from other neurons. Once input exceeds a critical level, the neuron discharges a spike - an electrical pulse that travels from the body, down the axon, to the next neuron(s) (or other receptors). This spiking event is also called depolarization, and is followed by a refractory period, during which the neuron is unable to fire.

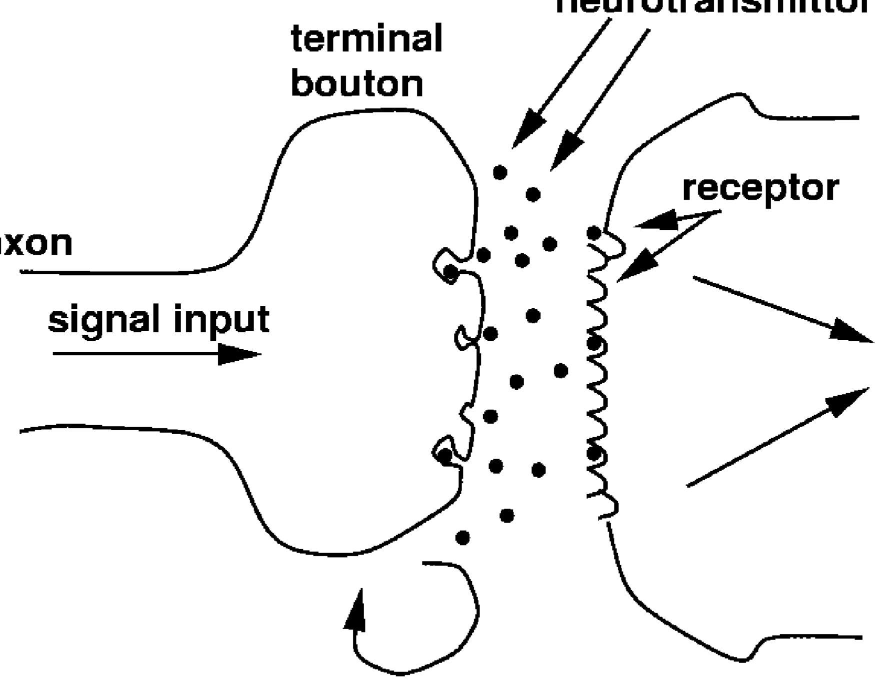
Neurons and Synapses

- The axon endings (Output Zone) almost touch the dendrites or cell body of the next neuron. Transmission of an electrical signal from one neuron to the next is effected by neurotransmittors, chemicals which are released from the first neuron and which bind to receptors in the second. This link is called a synapse. The extent to which the signal from one neuron is passed on to the next depends on many factors, e.g. the amount of neurotransmittor available, the number and arrangement of receptors, amount of neurotransmittor reabsorbed, etc.

Neurons and Synapses



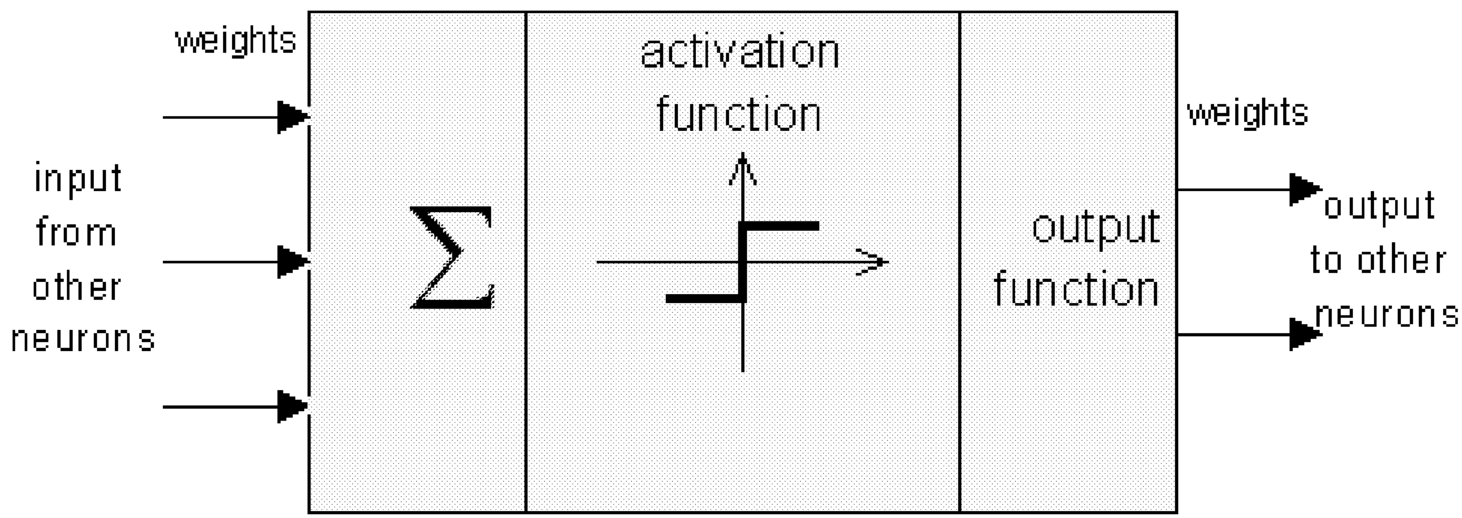
A Synapse



Neural System Characteristics

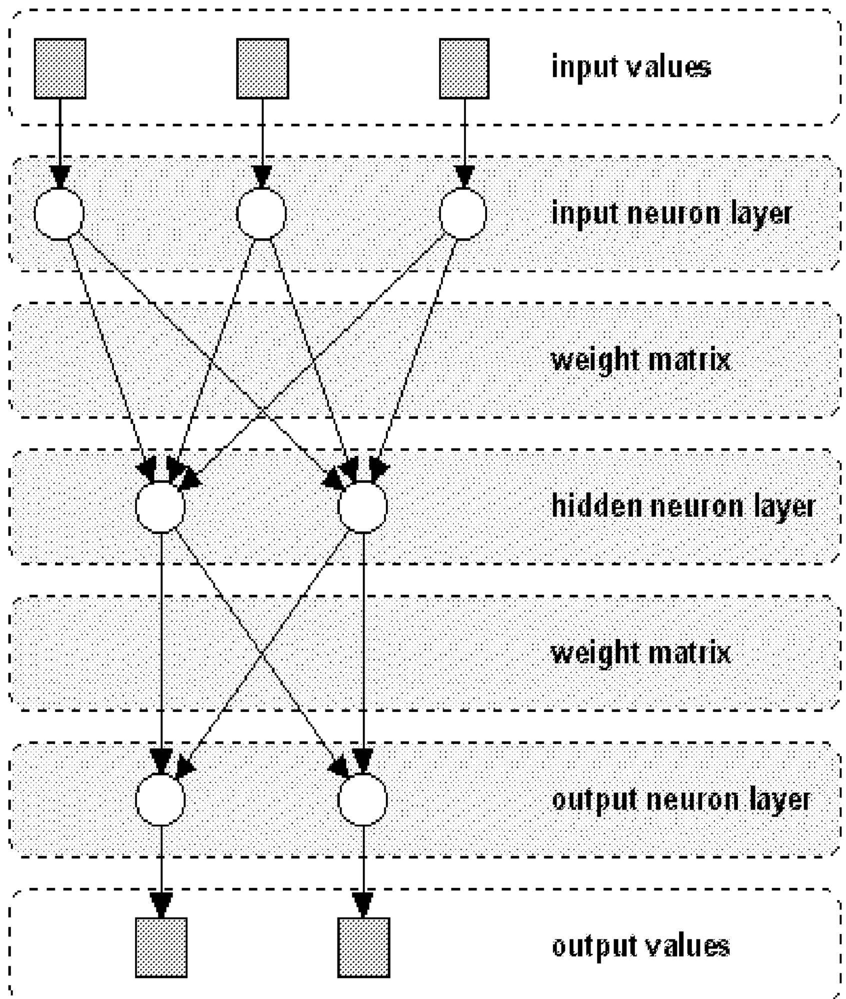
- parallel, distributed information processing
- high degree of connectivity among basic units
- connections are modifiable based on experience
- learning is a constant process, and usually unsupervised
- learning is based only on local information
- performance degrades gracefully if some units are removed (Fault Tolerant)

A Single Neuron



Structure of a neuron in a neural net

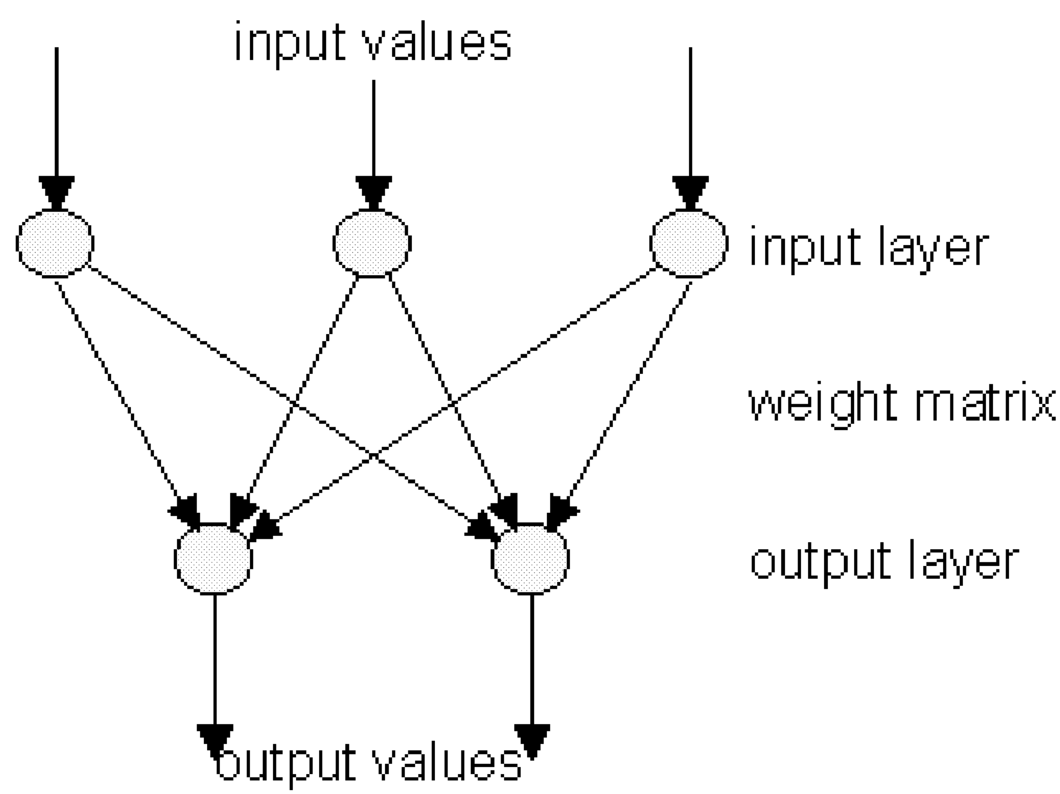
Three Layers Neural Network



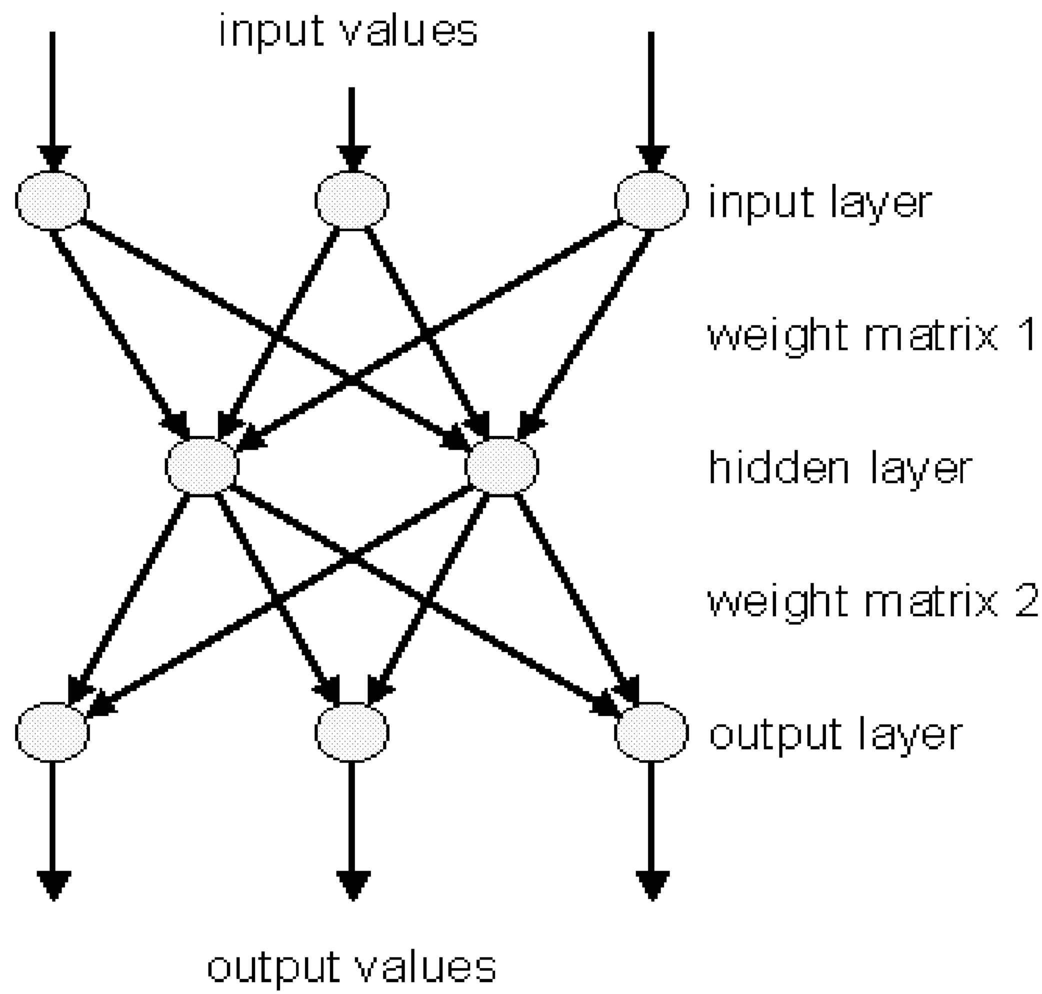
Neural Network Structures

- Perceptron
- Multi-Layer-Perceptron
- Backpropagation Net
- Hopfield Net
- Kohonen Feature Map

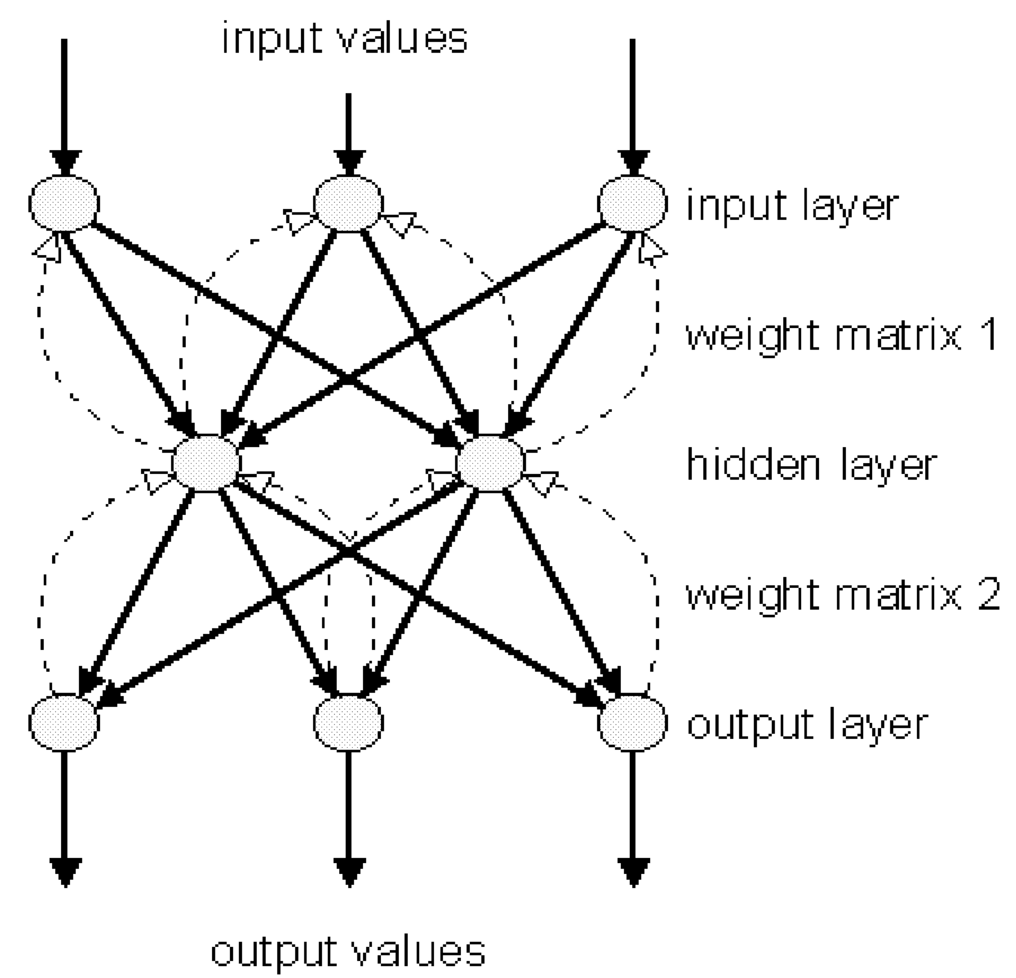
Perceptron Structure



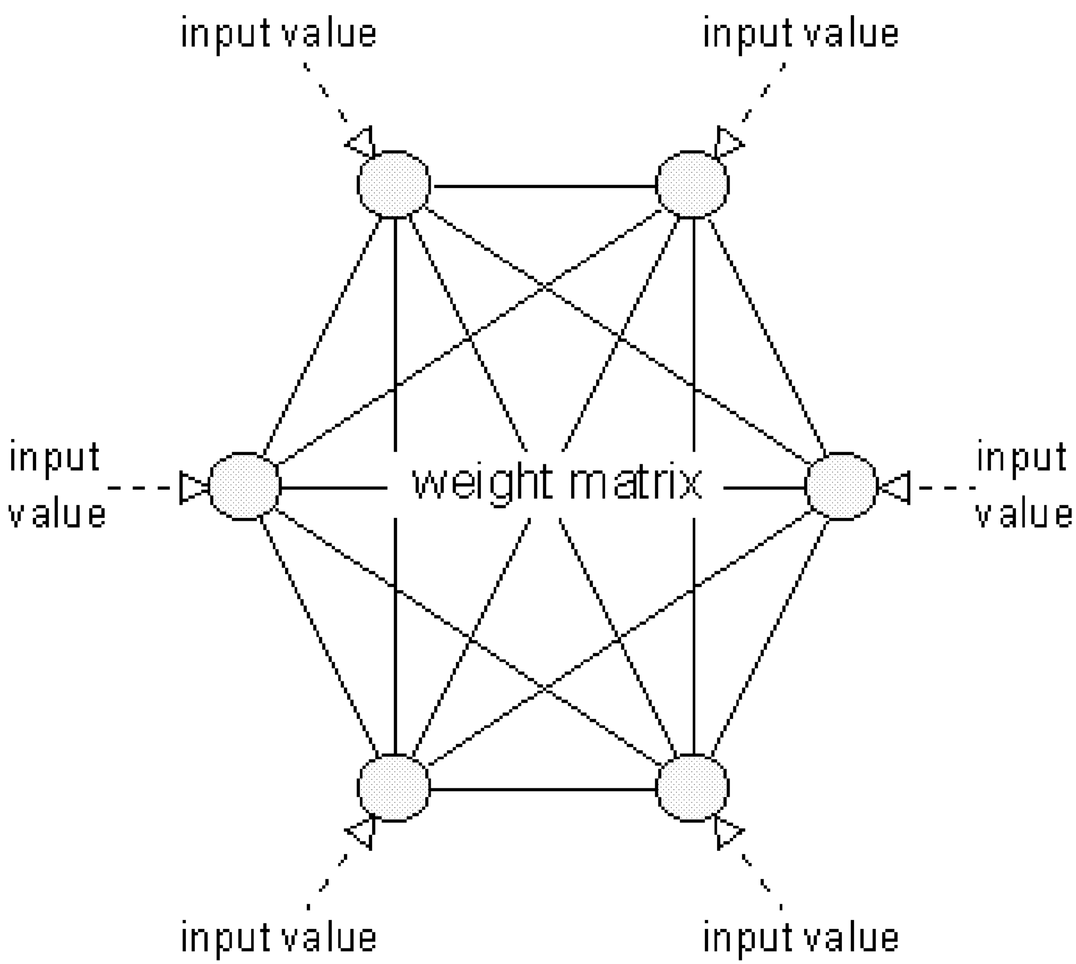
Multi-Layer-Perceptron Structure



Backpropagation Net Structure



Hopfield Net Structure



Kohonen Feature Map Structure